54

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,771	12/26/2001	Kazunori Aoyagi	04329.2712	5862

22852 7590 05/13/2005

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
RAMPURIA, SHARAD K	
ART UNIT	**PAPER NUMBER**
2683	

DATE MAILED: 05/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/025,771	**Applicant(s)** AOYAGI, KAZUNORI
	Examiner Sharad Rampuria	**Art Unit** 2683

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on *12 November 2004*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17,19 and 20* is/are pending in the application.

4a) Of the above claim(s) *18* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17,19 and 20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 November 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

Response to Amendment

Applicant's arguments with respect to claims 1-17, 19-20 have been considered but are moot in view of the new ground(s) of rejection.

Claim 18 is cancelled.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-17, & 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Oka [US 6091945] in view of Sugitani [JP 07162950 A].

1. Regarding claim 1, Oka disclose a communication apparatus (1; fig.6) comprising:
an authentication code storage section; (105; fig.6)
an authentication code updating section configured to calculate a new authentication code and update the authentication code stored in said authentication code storage section with the new authentication code when the authentication performed by said authentication section is successful; (Col.10; 8-21, 36-50, Col.13; 24-39) and

Oka fails to disclose configured to perform authentication of another communication apparatus. However, Sugitani teaches in an analogous art that an authentication section configured to perform authentication of another communication apparatus using an authentication code of the other communication apparatus stored in said authentication code storage section and the identification data of the other communication apparatus. (a wireless channel used to perform the communication between a first radio apparatus (main phone) connected to a communication network and at least one second radio apparatus (cordless handset). The second radio apparatus outputs an authentication signal encoded in a predetermined method based on **an authentication code** generated and outputted by the first radio apparatus, and **a password code** stored in the second radio apparatus. The first radio apparatus determines whether or not encoding of the authentication signal outputted by the second radio apparatus is correct **based on the password code and authentication code stored in the first radio apparatus**, and permits communication of the second radio apparatus, when the authentication code by the correct encoding is determined; Constitution) Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to include configured to perform authentication of another communication apparatus in order to provide the radio telephony system capable of lessening the risk of unauthorized use even when an ID code or an authentication code is plagiarized.

2. Regarding claim 2, Oka disclose The apparatus according to claim 1, further comprising: a comparator configured to compare an input authentication code with a predetermined authentication code; (Col.10; 8-21)

an ending section configured to end the authentication performed by said authentication section when both codes do not coincide with each other; (Col.10; 14-21) and

a starting section configured to operate said authentication section and said authentication code updating section when the both codes coincide with each other. (Col.10; 51-60)

3. Regarding claim 3, Oka disclose The apparatus according to claim 2, wherein said authentication section performs the authentication of the other communication apparatus using said input authentication code when the authentication code is not stored in said authentication code storage section. (Col.10; 8-21)

4. Regarding claim 4, Oka disclose The apparatus according to claim 2, wherein said authentication section performs the authentication of the other communication apparatus using identification data of the other communication apparatus and the authentication code which is the input authentication code when said authentication code storage section does not store authentication data of the other communication apparatus. (Col.10; 8-21)

5. Regarding claim 5, Oka disclose The apparatus according to claim 1, wherein said authentication section calculates authentication data based on identification data of the other communication apparatus and the authentication code and collates the calculated authentication data with authentication data of the other communication apparatus. (Col.10; 8-21)

6. Regarding claim 6, Oka disclose The apparatus according to claim 5, wherein said authentication section calculates the authentication data based on the identification data of the other communication apparatus, the authentication code and a random number. (Col.11; 49-63 & Col.18; 25-42)

7. Regarding claim 7, Oka disclose The apparatus according to claim 1, wherein said authentication code updating section subjects the authentication code stored in said authentication code storage section and used in the authentication to a predetermined calculation, and generates a new authentication code. (Col.10; 36-50 & Col.18; 43-51)

8. Regarding claim 8, Oka disclose The apparatus according to claim 7, wherein said authentication code updating section subjects the authentication code stored in said authentication code storage section and used in the authentication and a random number to the predetermined calculation, and generates the new authentication code. (Col.14; 43-52 & Col.18; 25-42)

9. Regarding claim 9, Oka disclose An authentication method between two communication apparatuses, comprising:

transmitting predetermined data to the apparatus to be authenticated from the apparatus demanding authentication;. (Col.9; 65-Col.10; 7)

comparing the obtained authentication data of both the apparatuses with each other in the apparatus demanding authentication; (Col.10; 8-21) and updating the authentication code for calculation in the two communication apparatuses based on the predetermined data and the authentication code for calculation when the authentication data of both the apparatuses coincide with each other. (Col.10; 36-50, Col.13; 24-39)

Oka fails to disclose calculating authentication data in the two communication apparatuses based on said predetermined data, an authentication code for calculation and of the apparatus to be authenticated. However, Sugitani teaches in an analogous art that calculating authentication data in the two communication apparatuses based on said predetermined data, an authentication code for calculation and of the apparatus to be authenticated, and identification data of the apparatus to be authenticated. (a wireless channel used to perform the communication between a first radio apparatus (main phone) connected to a communication network and at least one second radio apparatus (cordless handset). The second radio apparatus outputs an authentication signal encoded in a predetermined method based on **an authentication code** generated and outputted by the first radio apparatus, and **a password code** stored in the second radio apparatus. The first radio apparatus determines whether or not encoding of the authentication signal outputted by the second radio apparatus is correct **based on the password code and authentication code stored in the first radio apparatus**, and permits communication of the second radio apparatus, when the authentication code by the correct encoding is determined; Constitution) Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to include calculating authentication data in the two communication apparatuses based on said predetermined data, an authentication code for calculation and of the apparatus to be authenticated in order to provide the radio telephony system capable of lessening the risk of unauthorized use even when an ID code or an authentication code is plagiarized.

10. Regarding claim 10, Oka disclose The method according to claim 9, wherein an authentication code is input into each apparatus to be compared a predetermined authentication code and the authentication is ended when the input authentication code does not coincide with the predetermined authentication code. (Col.10; 8-21)

11. Regarding claim 11, Oka disclose The method according to claim 9, wherein an initial value of said authentication code for calculation is an input authentication code. (Col.10; 8-21)

12. Regarding claim 12, Oka disclose The method according to claim 9, wherein said predetermined data is a random number. (Col.11; 49-63 & Col.18; 25-42)

13. Regarding claim 13, Oka disclose A communication apparatus having a function for authenticating another communication apparatus (1; fig.6), comprising:
a comparator configured to compare an input first code or a prestored first code with a predetermined code; (Col.10; 8-21)
an ending section configured to end an authentication when the first code and the predetermined code do not coincide with each other; (Col.10; 14-21)
a transmitter configured to transmit a random number to the other communication apparatus when both of the first codes coincide with each other; (Col.11; 49-63 & Col.18; 25-42)

an updating section configured to update the authentication code based on the random number and the authentication code when both of the authentication data coincide with each other. (Col.10; 36-50)

Oka fails to disclose configured to perform a collation section configured to calculate authentication data based on the random number, an authentication code of the another communication apparatus. However, Sugitani teaches in an analogous art that a collation section configured to calculate authentication data based on the random number, an authentication code of the another communication apparatus, and identification data of the other communication apparatus, and collate the calculated authentication data with authentication data transmitted from the other communication apparatus. (a wireless channel used to perform the communication between a first radio apparatus (main phone) connected to a communication network and at least one second radio apparatus (cordless handset). The second radio apparatus outputs an authentication signal encoded in a predetermined method based on **an authentication code** generated and outputted by the first radio apparatus, and **a password code** stored in the second radio apparatus. The first radio apparatus determines whether or not encoding of the authentication signal outputted by the second radio apparatus is correct **based on the password code and authentication code stored in the first radio apparatus**, and permits communication of the second radio apparatus, when the authentication code by the correct encoding is determined; Constitution) Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to include a collation section configured to calculate authentication data based on the random number, an authentication code of the another communication apparatus in order to provide the radio telephony system capable of lessening the risk of unauthorized use even when an ID code or an authentication code is plagiarized.

14. Regarding claim 14, Oka disclose The apparatus according to claim 13, wherein said updated authentication code is stored in a storage section, and said collation section uses the input first code as the authentication code when the authentication code is not stored in the storage section. (Col.10; 8-21)

15. Regarding claim 15, Oka disclose a communication apparatus (1; fig.6) comprising:
a comparator configured to compare an input first code or a prestored first code with a predetermined code when authentication is requested by another communication apparatus; (Col.10; 8-21)
an ending section configured to end an authentication when the first code and the predetermined code do not coincide with each other; (Col.10; 14-21)
a receiver configured to receive a random number from the other communication apparatus;
an updating section configured to receive a result of authentication from the other communication apparatus and update the authentication code based on the random number and the authentication code when the authentication is successful. (Col.10; 36-50)

Oka fails to disclose a transmitter configured to calculate authentication data based on the random number, an authentication code of own apparatus, and identification data of own apparatus, and to transmit the calculated authentication data to the other communication apparatus. However, Sugitani teaches in an analogous art that a transmitter configured to calculate authentication data based on the random number, an authentication code of own apparatus, and identification data of own apparatus, and to transmit the calculated authentication data to the other communication apparatus. (a wireless channel used to perform the communication between a first radio apparatus (main phone) connected to a communication network and at least one second radio apparatus (cordless handset). The second radio apparatus outputs an authentication signal encoded in a predetermined method based on **an authentication code** generated and outputted by the first radio apparatus, and **a password code** stored in the second radio apparatus. The first radio apparatus determines whether or not encoding of the authentication signal outputted by the second radio apparatus is correct **based on the password code and authentication code stored in the first radio apparatus**, and permits communication of the second radio apparatus, when the authentication code by the correct encoding is determined; Constitution) Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to include a transmitter configured to calculate authentication data based on the random number, an authentication code of own apparatus, and identification data of own apparatus, and to transmit the calculated authentication data to the other communication apparatus in order to provide the radio telephony system capable of lessening the risk of unauthorized use even when an ID code or an authentication code is plagiarized.

16. Regarding claim 16, Oka disclose The apparatus according to claim 15, wherein said updated authentication code is stored in a storage section, and said transmission section uses the first code as the authentication code when the authentication code is not stored in the storage section. (Col.10; 8-21)

17. Regarding claim 17, Oka disclose an article of manufacture a computer usable medium having a computer readable program code embodied therein, the computer readable program comprising:

a first computer readable program code for causing a computer to allow two communication apparatuses authenticate each other using authentication code; (Col.10; 8-21) and

a second computer readable program code for causing a computer to calculate a new authentication code, and update the authentication code, when the authentication is successful. (Col.10; 36-50)

Oka fails to disclose to calculate authentication data based on an authentication code shared by the two communication apparatuses, identification data of one of the two communication apparatuses. However, Sugitani teaches in an analogous art that wherein the first program code causes a computer (a) to calculate authentication data based on an authentication code shared by the two communication apparatuses, identification data of one of the two communication apparatuses, and predetermined code generated by said one of the two communication apparatuses and transmitted to the other of the two communication apparatuses, and (b) to collate the authentication data of the two communication apparatuses. (a wireless channel used to perform the communication between a first radio apparatus (main phone) connected to a communication network and at least one second radio apparatus (cordless handset). The second radio apparatus outputs an authentication signal encoded in a predetermined method based on **an authentication code** generated and outputted by the first radio apparatus, and **a password code** stored in the second radio apparatus. The first radio apparatus determines whether or not encoding of the authentication signal outputted by the second radio apparatus is correct **based on the password code and authentication code stored in the first radio apparatus**, and permits communication of the second radio apparatus, when the authentication code by the correct encoding is determined; Constitution) Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to include to calculate authentication data based on an authentication code shared by the two communication apparatuses, identification data of one of the two communication apparatuses in order to provide the radio telephony system capable of lessening the risk of unauthorized use even when an ID code or an authentication code is plagiarized.

19. Regarding claim 19, Oka disclose a communication apparatus (1; fig.6) comprising:
an input section configured to input a first authentication code; (Col.9; 65-Col.10; 7)
an updating section configured to update the second authentication code of the external apparatus and corresponding to the first authentication code inputted by the input section and stored in the memory when the authentication by the authentication section is successful. (Col.10; 36-50)

Oka fails to disclose an authentication section configured to perform authentication for setting a communication link with an external apparatus using the second authentication code of the external apparatus and corresponding to the first authentication code inputted by the input section and read from the memory. However, Sugitani teaches in an analogous art that a memory which stores second authentication codes of other communication apparatuses corresponding to the first authentication code (memories 19; Constitution) an authentication section configured to perform authentication for setting a communication link with an external apparatus using the second authentication code of the external apparatus and corresponding to the first authentication code inputted by the input section and read from the memory. (a wireless channel used to perform the communication between a first radio apparatus (main phone) connected to a communication network and at least one second radio apparatus (cordless handset). The second radio apparatus outputs an authentication signal encoded in a predetermined method based on **an authentication code** generated and outputted by the first radio apparatus, and **a password code** stored in the second radio apparatus. The first radio apparatus determines whether or not encoding of the authentication signal outputted by the second radio apparatus is correct **based on the password code and authentication code stored in the first radio apparatus**, and permits communication of the second radio apparatus, when the authentication code by the correct encoding is determined; Constitution) Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to include an authentication section configured to perform authentication for setting a communication link with an external apparatus using the second authentication code of the external apparatus and corresponding to the first authentication code inputted by the input section and read from the memory in order to provide the radio telephony system capable of lessening the risk of unauthorized use even when an ID code or an authentication code is plagiarized.

20. Regarding claim 20, Oka disclose an authentication method of a communication apparatus comprising, (1; fig.6), the method comprising:
inputting the first authentication code; (Col.9; 65-Col.10; 7)

reading the second authentication code corresponding to the input first authentication code; (Col.10; 8-21)

updating the second authentication code of the external apparatus and corresponding to the first authentication code inputted by the input section and stored in the memory when the authentication is successful. (Col.10; 36-50)

Oka fails to disclose a memory which stores second authentication codes of other communication apparatuses corresponding to the first authentication code. However, Sugitani teaches in an analogous art that a memory (memories 19; Constitution) which stores second authentication codes of other communication apparatuses corresponding to the first authentication code and performing authentication for setting a communication link with an external apparatus using the output second authentication code (a wireless channel used to perform the communication between a first radio apparatus (main phone) connected to a communication network and at least one second radio apparatus (cordless handset). The second radio apparatus outputs an authentication signal encoded in a predetermined method based on **an authentication code** generated and outputted by the first radio apparatus, and **a password code** stored in the second radio apparatus. The first radio apparatus determines whether or not encoding of the authentication signal outputted by the second radio apparatus is correct **based on the password code and authentication code stored in the first radio apparatus**, and permits communication of the second radio apparatus, when the authentication code by the correct encoding is determined; Constitution) Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to include a memory which stores second authentication codes of other communication apparatuses corresponding to the first authentication code in order to provide the radio telephony system capable of lessening the risk of unauthorized use even when an ID code or an authentication code is plagiarized.

Conclusion

II. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Austin et al. [US 6393270] teaches an improved authentication method in cellular communication.

III. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sharad Rampuria whose telephone number is (571) 272-7870. The examiner can normally be reached on Mon-Fri. (8:10-4:40).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Trost can be reached on (571) 272-7872. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or *EBC@uspto.gov*.

Sharad Rampuria
Examiner
Art Unit 2683

4 May 2005

WILLIAM TROST
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600